資料２－４－２

2018 年 1 月 1 日以降始期契約用

サイバーセキュリティ総合補償プラン　ヒアリングシート

ヒアリング実施日	年　　月　　日
ヒアリング相手	
作成者	

各質問事項にご回答下さい。

No.	ご質問事項	ご回答内容		
1	セキュリティポリシー、または情報セキュリティポリシーを策定している。	YES		NO
	上記が「YES」の場合、下記もご回答ください。			
	セキュリティ対策を所管する部門があり、監査体制も整っている。	YES		NO
	セキュリティの社内教育・研修・訓練を定期的（年1回以上）に実施している。	YES		NO
	パート、派遣社員等を含む使用人に、情報の取扱いに関する誓約書（情報保護の義務、そしてその義務違反時の損害賠償を定めたもの）の提出を要請している。 またはセキュリティ事故が発生した場合の、発生させた本人に対する罰則を定めた社内規定がある。	YES		NO
2	社内ネットワーク(イントラネット)では、機密情報を区分･特定し、そのダウンロード、アクセスは特定の権限者に制限し、暗号化などで保護している。	YES	制限のみ実施	NO
	上記が「YES」、または「制限のみ実施」の場合、下記もご回答ください。			
	機密情報のダウンロード、アクセスについてログを一定期間保存している。	YES		NO
3	クレジットカード（提携カードを含む）またはキャッシング機能を有するカードの発行を行っている。	YES		NO
4	社内では ID カードなどの身分証明書の着用を義務づけている。	YES	行っているが不完全	NO
5	外来者との応対は、執務場所を通過しないようにし、かつ、応対場所はゾーニング（区分け）している。	YES	一部実施	NO
6	外部と接続するサーバー等には、ファイアウォールや IDS が最新の状態で導入されている。	YES	最新ではないが導入	NO
7	社内と社外間のネットワークへのアクセスおよび社内ネットワークから外部へのアクセスについて、最低 3 か月以上ログを保存し、定期的に分析・監視している。	YES		NO
8	パソコン、サーバーには、ウイルス対策ソフトおよび OS のセキュリティ上の脆弱性に対する修正プログラム（セキュリティパッチ）が最新の状態で導入されている。	YES	最新ではないが導入	NO
9	E メールに関して、フィルタリングや暗号化を実施している。	YES		NO
10	ネットワーク上の通信は暗号化している。	YES	一部実施	NO
11	ISO/IEC15408 の認証が付与された OA 機器またはシステムを導入使用している。	YES		NO
12	退職者の ID やパスワードを遅滞なく無効化・削除している。	YES		NO
13	情報セキュリティに関して外部業者による監査を定期的に（年1回以上）実施している。	YES		NO
14	災害や障害の発生時における業務の復旧、データのバックアップなど危機管理対策が策定されている。	YES		NO
15	情報の取扱いの全部または一部、または情報の廃棄処理を、外部に委託または外部から受託している。	YES	時々ある	NO
	上記が「YES」または「時々ある」の場合、下記もご回答ください。			
	契約書には、「秘密保持」「再委託禁止」「損害賠償」「委託終了時の返却方法」が規定されている。	YES	一部規定	NO

No.	ご質問事項	ご回答内容		
16	個人情報など管理すべき情報の保管場所は、施錠管理がされており、入退室は許可者に限定され、かつ、入室者等は記録されている。	YES	一部実施	NO
17	情報の廃棄時には、再利用不可となるよう適切な処理を行い、その記録を保存している。 外部業者へ廃棄を委託する場合は、その外部業者から報告書を保管している。	YES		NO
18	ノートパソコンや、USB メモリ、DVD-R 等の記録媒体に保存されたデータを社外に持ち出せないようにしている。 または、これらを持ち出す際には、第三者が容易に情報を読み取ることができないようデータの暗号化やパスワード設定するなどの対策を行っている。	YES	一部実施	NO
19	パソコン、サーバー上の情報について、USB メモリ、DVD-R 等の記録媒体へのコピー制限、プリンタへの印刷制限、またはプリンタへの印刷時に印刷者の特定ができるソフト等を導入している。	YES	一部実施	NO
20	情報セキュリティ管理を委託している特定の情報セキュリティ業者がいる。	YES		NO
21	ウイルス情報、不正アクセス情報、インシデントがあった場合に IPA への届出や JPCERT への情報提供、その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している。	YES		NO
22	貴社および貴社グループ企業以外の第三者が使用することを目的としたネットワーク・ECサイトは構築していない。	YES		NO
23	情報セキュリティに関する事故に対する、具体的な手順フローを定め、ネット遮断等を含めた対応につき、期限をもって責任者が判断する体制を構築している。	YES		NO
	上記が「YES」の場合、下記もご回答ください。			
	情報セキュリティに関する事故収束後の再発防止策の策定も含めて、定期的に対応訓練や演習を行っている。	YES		NO
24	CISO（Chief Information Security Officer：最高情報セキュリティ責任者）を置いている。	YES		NO
25	CSIRT（Computer Security Incident Response Team）または SOC（Security Operation Center）を構築している。	YES		NO
26	社内ネットワーク上に Windows-XP 等、サポートが終了している OS を使用している端末は存在しない。または存在する場合であっても、セキュリティベンダ等から提供されるアップデート・パッチ対応を遅滞なく行っている。	YES		NO
27	社員の私有端末の業務利用(BYOD：Bring your own device)を認めていない。 または、認めている場合であっても、顧客情報へのアクセス・保存の禁止およびその他のセキュリティ対策を十分に実施している。	YES		NO
28	取得している認証にチェックしてください。 ☐ TRUSTe マーク …Web サイト・携帯サイトに関する個人情報保護の認証制度。認証付与機関は日本プライバシー認証機構。 ☐ プライバシーマーク制度 …個人情報保護に関する認証制度。認証付与機関は JIPDEC（日本情報経済社会推進協会） ☐ ISMS 認証 …情報セキュリティマネジメントシステムを適切に保持しているかどうかの認証制度(JIPDEC が定める適合性評価制度）。 ☐ BS7799 …英国規格協会による情報セキュリティマネジメントシステムに関する規格 SECURITY ACTION …独立行政法人情報処理推進機構が運営する情報セキュリティ対策に関する制度。 ☐ 一つ星ロゴマーク ☐ 二つ星ロゴマーク			
29	導入しているソフトウェア・システムにチェックしてください。 ☐ URL(WEB)フィルタリングソフト ☐ IPS（Intrusion Prevention System） ☐ WAF(Web Application Firewall) ☐ C&C サーバーとの通信を遮断する機能を有する機器・ソフトウェア ☐ パターンファイル型のウイルス検知ソフト以外に振る舞い検知を行う機器・ソフトウェア			

No.	ご質問事項	ご回答内容	
30	貴社のデータが保管されるデータセンターまたはサーバ等の設置・保管場所の名称・住所を記入してください。 データの保管場所が複数ある場合には、すべての所在地を記入してください。	所在地名称: 住所:	
31	現時点から起算して過去 3 年間において、サイバーリスクに伴う事故が発生し、喪失利益や営業を継続するための費用が発生したことがありますか？	YES	NO
	上記が「YES」の場合、下記もご回答ください。		
	次の①～④の事項をご申告ください。 複数存在する場合には、各々の事由につき別紙にご記入ください。 ① 発生した年月 ② 内容 ③ 貴社に発生した喪失利益の額 ④ 貴社が負担した営業を継続するための費用		

以上